REMARKS

This Amendment is filed in response to the Office Action mailed on June 4, 2003. All objections and rejections are respectfully traversed.

Claims 1-53 are in the case.

Claims 50-53 were added to better claim the invention.

Numerous claims were amended to better claim the invention.

At paragraph 2 of the Office Action it is indicated that new grounds of rejection are set out in the Office Actin.

At paragraph 3 of the Office Action the "101 rejection" of claim 34 is repeated, with the provision that:

> "Amending the claim so that it covers a computer network on which electromagnetic signals propagate would overcome this rejection."

Applicant respectfully points out that the preamble of Claim 34 recites a "computer network" in the form:

> 34. Electromagnetic signals ***propagating on a computer network***, comprising:
> said electromagnetic signals carrying instructions for execution on a processor for the practice of the method of,
> providing a tightly-coupling hardware data encryption function with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch;
> providing an encryption execution unit within the pipelined processor;
> enabling, by an ALU in response to reading an op-code, the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the memory; and
> selecting as output the result of processing by the encryption execution unit rather than selecting results from the ALU.

Applicant respectfully urges that the electromagnetic signals, as claimed, are tangible because they ***propagate on a computer network***, as required by the Examiner.

At paragraph 4 of the Office Action it is asserted that the arguments presented in the Amendment filed on March 13, 2002, do not apply to claim 20.

The invention, according to representative claim 20, comprises in part:

> 20. A programmable processing engine of a network switch comprising:
> an input header buffer;
> an output header buffer; and

a plurality of processing complex elements symmetrically arrayed into rows and columns that are embedded between the input header buffer and an output header buffer, each processing complex element comprising a microcontroller core having an encryption tightly coupled state machine (TCSM) unit that is selectively invoked in response to the microcontroller reading an op-code; and

a selector to select an output from either the microcontroller OR the TCSM.

The argument set out on the basis of representative claim 1 in the Amendment filed on March 13, 2003, were based on the representation of the invention set out in representative claim 1.

Further, Applicant points out that none of the cited art addressed by the Amendment filed on March 13, 2003, teaches Applicants claimed ***a selector to select an output from either the microcontroller OR the TCSM*** . Accordingly, Applicant respectfully urges that the invention, as set out in representative claim 20, is patentable in view of all art treated in the March 13, 2003, Amendment.

At paragraph 5 of the Office Action claims 33 and 34 were objected to under 35 CFR 1.75(c). Accordingly, claims 33 and 34 were written with the method steps of claim 10. New claims 50-53 were added for computer readable media and electromagnetic signals with the method steps of claims 27 and 40.

At paragraph 6 of the Office Action claims 20, 21, 27, 35, 40, 41, 44, 45, and 49 were objected to because they recite "OR". A logical OR is intended, and is indicated by the capitalization of the word "OR". Applicant respectfully urges that a claim having a logical "or" is a proper claim format.

Also, at paragraph 6 of the Office Action claim 21 was objected to as requiring a "to". Claim 21 was accordingly amended.

Also, at paragraph 6 of the Office Action claim 27 was objected to as in the fifth line of the claim, the word "should be process", not "process". Claim 27 was accordingly amended.

Also, at paragraph 6 of the Office Action claim 5 was objected to as needing an "a" after "is" in the first line. Claim 5 was accordingly amended.

Also, at paragraph 6 of the Office Action claim 32 was objected to as "Initialing" should be "initalizing". Claim 32 was accordingly amended.

Also, at paragraph 6 of the Office Action claim 23 was objected to as needing an "s" at the end of the last word of the first line. Claim 23 was accordingly amended.

Also, at paragraph 6 of the Office Action claim 28 was objected to as needing an "s" at the end of "comprise". Claim 28 was accordingly amended.

At paragraphs 7-8 of the Office Action claims 1-19 and 21-49 were rejected under 35 U.S.C. 112, first paragraph, on the grounds that the "specification does not teach an ALU enabling or transferring processing to an encryption execution unit".

At page 5, lines 21-page 6 line 4, a tightly coupled state machine for processing, including encryption, is described as:

> The novel encryption execution unit is preferably a specialized encryption *tightly coupled state machine* (TCSM) unit that is selectively invoked within the execution stage. In response to decode processing of the native opcodes, the encryption TCSM unit is invoked to perform encryption/decryption functions that utilize the hardware interface of the processor to access the processor's resources, including a plurality of high-performance internal busses that faciliate overlapping of operations. For instance, the encryption TCSM unit can simultaneously load an encryption key while storing a previous encryption result. Overlapping of operations improves encryption throughput by further reducing latency typically associated with a conventional encryption hardware module attached to a processor's external bus.

Further, at page 13 line 1 - 11 the novel TCSM is further described as:

> Fig. 7 is a schematic diagram of the TMC core 700 which preferably embodies a multi-stage pipeline data path organization comprising (i) an instruction fetch (IF) stage 710; (ii) an instruction decode (ID) stage 720; (iii) an execution (EX) stage 730; and (iv) a memory write-back

> (MW) stage 740. A plurality of interstage registers ISR1A 722 and ISR1B 724 are used with the ID stage, while an ALU 732 and a TCSM 734 are used in the EX stage. According to the TMC micro-architecture, memory operands are stored in ISR1B and provided to the B sides of the ALU and TCSM, whereas intermediate operands are stored in ISR1A and provided to the A sides of those logic units. Another interstage register ISR2 744 is provided at the MW stage for data that is destined for the local bus 525; for instructions that specify the internal register file as the destination of the data, the write-back actually occurs during the EX stage.

The use of the TCSM as an encryption processor is described in the specification at page 14 line 1-line 23 as:

> Specifically, the invention relates to an encryption mechanism that tightly-couples hardware data encryption functions with software-based protocol decode processing within the TMC processor core 700. Tight-coupling is achieved by the TMC micro-architecture which allows encryption functions to be accessed as a novel *encryption TCSM unit* of the TMC. Such coupling substantially reduces the latency associated with conventional hardware/software interfaces. Additional mechanisms, such as branch instructions, enable the software executing on the processor to receive encryption status information (i.e., completion status) in an efficient manner.
>
> Increased processing performance is realized by, *inter alia*, a reduction in latency and bandwidth consumption when migrating between protocol decode (which is a precursor to encryption) and encryption operations. For example, once the TMC processor finishes protocol decoding, or at least proceeds far enough to realize encryption/decryption is required, it can immediately start a DMA operation to fetch the initial keys needed for encryption/decryption. Upon fetching the keys, the required data is localized within the processor, which obviates the need for data transfers over the local bus and across external interface boundaries.
>
> In the illustrative embodiment, the novel TCSM unit executes a conventional DES encryption/decryption algorithm as defined by *National Bureau of Standards Data Encryption Standard*, Federal Information Processing Standards Publication 46-1, January 22, 1988; however, it should be noted that other data encryption algorithms, such as public key encryption algorithms, may be used in accordance with the principles dis-

cussed herein. Broadly stated, encryption of data according to the DES algorithm entails the following steps:

The TMC core 700 (Fig. 5) is described in the text cited above as selecting the tightly coupled state machine, is further shown in Fig. 7 to have an ALU 732, a TCSM 734, and a multiplexer 742 controlled by the ALU. The ALU 732 controls the multiplexer 742 to select an output from either the ALU or the TCSM, as claimed.

Accordingly, Applicant respectfully urges that the description in the Specification of detailed operation of the ALU 732, TCSM 734, and MUX 744 meet all requirements of 35 U.S.C. § 112 first paragraph.

At paragraphs 9 of the Office Action, 35 U.S.C. 112, second paragraph is mentioned.

At paragraph 10-11 of the Office Action, claims 1-9, 11-19 are rejected under 35 U.S.C. 112 second paragraph on the grounds that, in Claim 1 “the limitation ‘the result’ in the second to last line of the claim, should have “the” changed to “a”. Claim 1 is accordingly amended.

At paragraph 12 of the Office Action Claim 3 is rejected because “the interface” in its first line lacks antecedent basis. Amended of claim 3 is believed to satisfy this rejection.

At paragraph 13 of the Office Action, claim 4 was rejected on the grounds that “the resources” recited in the first line lacks antecedent basis. Amendment of claim 4 is believed to satisfy this rejection.

At paragraph 14 of the Office Action, claims 9 and 26 were rejected because they “recite ‘the DES function’, and “there is insufficient antecedent basis for this limitation”. Amendment of the claims is believed to satisfy this rejection.

At paragraph 15 of the Office Action claim 11 was rejected because it recites “the integrated interface” in the first line; “the step of selectively accessing” in lines 2 and 3; and the step “the step of issuing” in line 3, on the grounds of insufficient antecedent basis. Amendment of claim 11 is believed to satisfy this rejection.

At paragraph 16 of the Office Action claim 14 was rejected because it recites “the resources”, and there is insufficient antecedent basis. Amendment of claim 16 is believed to satisfy this rejection.

At paragraph 17 of the Office Action claim 18 was rejected because it recites "the plaintext", and there is insufficient antecedent basis. Amendment of claim 18 is believed to satisfy this rejection.

At paragraph 18 of the Office Action claim 23 was rejected because it recites "the one or more internal registers" in the third line lack sufficient antecedent basis. Amendment of claim 23 is believed to satisfy this rejection.

At paragraph 19 of the Office Action claim 30 was rejected because it recites "the DES functional component" at lines 3 and 4; "the sub-key generation functional component" on lines 5-6, and there is insufficient antecedent basis. Amendment of claim 30 is believed to satisfy this rejection.

At paragraph 20 of the Office Action claim 31 was rejected because it recites "the sub-key generation functional component" in line 3, and there is insufficient antecedent basis. Amendment of claim 31 is believed to satisfy this rejection.

At paragraph 21 of the Office Action, claim 32 was rejected because it recites "the DES operations", and there is insufficient antecedent basis. Amendment of claim 32 is believed to satisfy this rejection.

At paragraph 22 of the Office Action claim 34 was rejected under 35 U.S.C. § 101, on the grounds that "data structures must be tangibly embodied to be statutory".

Applicant respectfully points that computer readable media are patentable subject matter under 35 U.S.C. § 101. Computer readable media are memory such as RAM memory, magnetic discs, etc., and are physically embodied, as required by the Examiner.

At paragraph 23-24 of the Office Action claims 1-19 and 21-49 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hawe et al. in vies of Chi et al., Johns-Vano et al., Farrell et al., Narad et al., Schneier, and the Microsoft Press Computer Dictionary.

This cited art is, more particularly:

Hawe et al. US Patent Number 5,070,528 issued December 3, 1991 (hereinafter Hawe).

□

Chi et al. US Patent Number 5,706,489 issued January 6, 1989 (hereinafter Chi).

Johns-Vano et al. U.S. Patent Number 6,026,490 issued February 15, 2000 (hereinafter Johns-Vano).

Farrell et al. U.S. Patent Number 5,182,800 issued January 26, 1993 (hereinafter Farrell).

Narad et al. U. S. Patent No. 6,157,955 (hereinafter Narad).

Bruce Schneier, "Applied Cryptography, second edition" published 1996, John Wiley & Sons, Copyright 1996 (hereinafter Schneier).

"Microsoft Computer Dictionary, third edition", Copyright 1997 (hereinafter Microsoft Computer Dictionary).

The invention, as set out in representative claim 1, comprises in part:

> 1. Apparatus for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the apparatus comprising:
>
> an encryption execution unit contained within the pipelined processor;
>
> ***an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the shared memory; and***
>
> ***a multiplexer to select as an output a result of processing by the encryption execution unit rather than a result of ALU processing.***

Applicant respectfully points out that the cited art has been previously characterized in various Amendments.

The cited patents have been characterized in former amendments as follows:

Hawe was discussed in the Amendment filed on 3/13/03 as follows.

Hawe et al., discloses a cryptographic processing unit which connects to a MAC interface so that the cryptographic unit can either receive packets as they are received from a network at the MAC interface, or as they stream to the MAC interface for transmission onto the network. The cryptographic unit may be bypassed by a multiplexer if a packet does not require treatment by the cryptographic unit.

Hawe was discussed in the Amendment filed on 10/9/03 as follows.

Hawe discloses a cryptographic processing unit which connects to a MAC interface so that the cryptographic unit can either receive packets as they are received from a network at the MAC interface, or as they stream to the MAC interface for transmission onto the network. The cryptographic unit may be bypassed by a multiplexer if a packet does not require treatment by the cryptographic unit.

Chi was discussed in the Amendment filed on 3/13/03 as follows.

Chi discloses a processor, which uses a parallel instruction execution unit (PIE) so that the processor can offload computationally intense processing to the PIE. The processor executes an instruction which transfers a parallel instruction execution parameter block (PPB) to the PIE. The processor and the PIE facility share RAM storage, and the PIE facility can execute code read from the RAM storage beginning at a location specified in the PPB header. Accordingly, the PIE facility may be used to perform data base record expansion, may perform encryption, data conversion, etc. The PIE performs one sequence of instructions while the processor continues executing another sequence of instructions. (Col. 2, lines 48-52)

Johns-Vano was discussed in the Amendment filed on 3/13/03 as follows.

Johns-Vano discloses a cryptographic processor 100, where the cryptographic processor is controlled by external controller 10 and is provided data from external memory 12. Further, microcode memory 200 stores different sets of microcode which may be transferred over bus 104 to microsequencer 302, depending upon the job that cryptographic processor 100 is requested to perform (column 2 lines 48-54). Accordingly, cryptographic processor 100 may be initialized to perform a variety of requests, as set out in column 3 lines 26-61. Further, the header of a data unit is processed, and depending upon the channel program that directs the microsequencer, the data is copied from the external memory 12 to a specified destination location, after set up of the cryptographic processor has been completed (column 7 lines 35-58).

Johns-Vano was discussed in the Amendment filed on 10/09/03 as follows.

Johns-Vano discloses a cryptographic processing engine which can process two cryptographic algorithms by background staging and algorithm multi-tasking. A three stage pipeline is used.

Farrell was discussed in the Amendment filed on 3/13/03 as follows.

Farrell discloses a direct memory access controller which provides some pipelining between units attempting to arbitrate for bus 2c. Time constraints on bus 2c are addressed by the Farrell disclosure by using a direct memory access controller memory in conjunction with an additional FIFO memory. The direct memory access controller also contains a tightly coupled state machine (column 16 lines 60-63), where the state machine 84 (Fig. 8) assists in operation of the direct memory access function.

Farrell was discussed in the Amendment filed on 10/09/03 as follows.

Farrell discloses a multi-channel direct memory access controller using adaptive pipelining.

Narad was discussed in the Amendment filed on 10/09/03 as follows.

Narad discloses a network infrastructure which separates classification and action. Narad's overall architecture is shown in his Fig. 3. Some of Narad's timing is shown in his Fig. 14.

Narad was discussed in the Amendment filed on 1/18/02 as follows.

The Narad patent describes a packet-processing system that accelerates network infrastructure applications by employing a three-tier approach to filtering packets (col. 7, lines 7-10). Packets are first run through a classification engine that executes hardware assist operations such as chained field comparisons (col. 6, lines 62-66). Packets are then handed to a policy processor, a microprocessor that executes policy decisions such as to pass, drop, enqueue, etc... (col. 6 line 66 to col. 7, line 2). Packets that require additional processing are sent to an application processor, a general purpose microprocessor (col. 7, lines 2-4 and col. 3, lines 66-67) and/or an external cryptography ("Crypto") co-processor (col. 8, lines 1-2 and col. 26 lines 65-67 and Fig. 3, item 246). The Crypto co-processor obtains packets from a buffer, performs its operation, and then writes the result to back to a memory address (col. 27, lines 10-29).

Applicant respectfully urges that Narad does not show Applicant's claimed novel "encryption execution unit contained within the pipelined processor."

The Narad patent describes the Crypto co-processor as an external and separate processor. There is absolutely no disclosure of including the Crypto unit within another processor that performs protocol decode functions. Further, because the Crypto unit is located externally and reads and writes from internal buffers and memory, substantial data movement must occur over system buses. This particular limitation is novelly overcome by the Applicant's design.

Applicant respectfully urges that none of the cited art discloses Applicant's claimed novel

an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the shared memory; and

a multiplexer to select as an output a result of processing by the encryption execution unit rather than a result of ALU processing.

Applicant respectfully urges that the absence from all cited art of Applicant's claimed ALU and multiplexer legally precludes any combinatin of the cited art from rendering Applicant's claimed invention obvious under 35 U.S.C. § 103(a).

At paragraph 25 of the Office Action claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Farrell et al., in view of Chi et al., and Narad et al.

The invention, as set out in representative claim 20, comprises in part:

20. A programmable processing engine of a network switch comprising:
an input header buffer;
an output header buffer; and
a plurality of processing complex elements symmetrically arrayed into rows and columns that are embedded between the input header buffer and an output header buffer, each processing complex element comprising a microcontroller core having an encryption tightly coupled state machine (TCSM) unit that is selectively invoked in response to the microcontroller reading an op-code; and
a selector to select an output from either the microcontroller OR the TCSM.

Applicant respectfully urges that neither Farrell, Chi, nor Narad disclose Applicants claimed novel

a plurality of processing complex elements symmetrically arrayed into rows and columns that are embedded between the input header buffer and an output header buffer, each processing complex element comprising a microcontroller core having an encryption tightly coupled state machine (TCSM) unit that is selectively invoked in response to the microcontroller reading an op-code; and

a selector to select an output from either the microcontroller OR the TCSM.

In particular, Applicant respectfully points out that none of the cited art discloses Applicants claimed novel ***a selector to select an output from either the microcontroller OR the TCSM***.

Accordingly, Applicant respectfully urges that the absence from all cited art of Applicant's claimed novel ***a selector to select an output from either the microcontroller OR the TCSM*** legally precludes any combination of the cited art from rendering Applicant's claimed invention obvious under 35 U.S.C. § 103(a).

Even further, an analysis under *Graham v. Deere*, 383 U.S. 1, 148 U.S.P.Q. 459, (1966), and cited in MPEP 706.02 (m), comes to the same conclusion, that the claimed invention is novel and non-obvious. The three analytic criteria under *Graham v. Deer* are:

1. Determining the scope and content of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

Further, objective evidence present in the application indicating obviousness or nonobviousness is considered.

Using these analytic criteria, one then makes a legal determination as to whether or not a person of ordinary skill in the pertinent art would have found the claimed invention obvious at the time that the invention was made.

First, the scope and content of the prior art is determined by reference to the cited art, Hawe, Chi, Johns-Vano, Farrell, Narad, Schneier, and the "Microsoft Computer Dictionary". The scope and content of the prior art is summarized as: Hawe discloses an encryption unit with a straight bypass; Chi discloses a parallel execution unit (PIE) which competes with a controlling processor for a common memory; Johns-Vano discloses a cryptographic processor with an extensive set-up time; and Farrell teaches a direct memory access controller using a plurality of state machines.

2. The differences between the claimed invention and the cited art are, as set out in the claimed novel invention:

an ALU, in response to reading an op-code, enables the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the shared memory; and

a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing.

Particularly, there is no mention of Applicants use of ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing*** in any of the cited art, Hawe, Chi, Johns-Vano, Farrell, Narad, Schneier, and the "Microsoft Computer Dictionary".

Applicant respectfully urges that none of the cited art show ***a multiplexer to select as an output the result of processing by the encryption execution unit rather than a result of ALU processing***.

Further, as set out in Claim 20, Applicant respectfully urges that the absence from all cited art of Applicant's claimed novel ***a selector to select an output from either the microcontroller OR the TCSM*** legally precludes any combination of the cited art from rendering Applicant's claimed invention obvious under 35 U.S.C. § 103(a).

3. The level of ordinary skill in the art of computer architecture can be ascertained by reference to the cited art, Hawe, Chi, Johns-Vano, Farrell, Narad, Schneier, and the "Microsoft Computer Dictionary". As pointed out hereinabove, each of these cited documents, taken either singly or in any combinatin, teach away from the presently claimed invention. Accordingly, the level of skill taught by the prior art is totally inadequate to render the presently claimed invention obvious.

Accordingly, it must be concluded that the state of the art before the invention was made is that a parallel execution unit is either bypassed (Hawe), or competes with a controlling processor for a common memory (Chi, Johns-Vano), or that state machines are only used in direct memory access controllers.

Accordingly, the legal conclusion which is required by the application of the *Graham v. Deere* analytic method, is that a person of ordinary skill in the art of the cited art (Hawe, Chi, Johns-Vano, Farrell, Narad, Schneier, and the "Microsoft Computer Dictionary") could not have found the present invention obvious, because of the absence of the claimed elements of the presently claimed invention in all of the cited art.

All independent claims are believed to be in condition for allowance.

All dependent claims are believed to be dependent from allowable independent claims, and therefore in condition for allowance.

Favorable action is respectfully solicited.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

A. Sidney Johnston

A. Sidney Johnston
Reg. No. 29,548
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500